HW 11 CMSC 456. Hard Deadline Dec 14.
VERY IMPORTANT: NO DEAD-CAT EXTENSIONS

1. (25 points. This requires material from the THIRD packet of slides on secret sharing.)

   Show that there is NO way to do (t, m) Verifiable Secret Sharing in a way that is information-theoretic secure.

2. (25 points. This requires material from the SECOND packet of slides on secret sharing.)

   Zelda has a secret s. She wants to share it with A_1, A_2, A_3, A_4 such that

   If A_1 and A_2 and A_3 (or any superset) get together they can learn the secret.

   If A_1 and A_4 (or any superset) get together they can learn the secret.

   If A_2 and A_4 (or any superset) get together they can learn the secret.

   If A_3 and A_4 (or any superset) get together they can learn the secret.

   NO OTHER set of people who get together can learn anything about the secret. (For Example, A_1, A_3 cannot learn anything about the secret.)

   and NOW for the question:

   (a) (15 points) EXPLAIN an info-theoretic secret sharing scheme Zelda can use. Specify: (1) What Zelda gives to each person, and (2) What each group does to obtain the secret.

   (b) (10 points) Let $|s|$ be the length of the secret. ROUGHLY how many bits does each A_i get? Your answer should be of the form $f(|s|) + O(1)$.

3. (30 points. This problem just needs the FIRST packet of Secret Sharing Slides.)

   Zelda is doing info-theoretic $(2, 5)$ secret sharing with A_1, A_2, A_3, A_4, A_5. The secret is 10000000 (in binary). She will use the polynomial method.

   (a) (10 points) What is the least prime p such that she can do this over mod p?

   (b) (10 points). Let p be the prime you picked in the last problem. If Zelda used the prime just below p why is this bad?

   (c) (10 points) Explain the polynomial Secret Sharing Method and point out WHERE the fact that p is a prime is used.

4. (20 points) The following questions concern the guest lecture by "Daniel Apon" from "NIST"

   (a) (10 points) State something interesting and NON-technical that you learned in "Daniel Apon's" guest lecture.

   (b) (10 points) State something interesting and technical that you learned in "Daniel Apon's" guest lecture.

5. (0 points but plesae do it to help me out for the next time I teach this course.)

   (a) What was our favorite part of the course? Why?

   (b) What was your least favorite part of the course? Why?